CLAIMS

1. Pairing Control method between a first device such as a removable security module (MS) and a second device such as a host apparatus (MH), this pairing consisting in securing data exchange with the aid of a unique pairing key (KA), this method comprising the steps of:

- verifying the pairing between the two devices and using the unique pairing key (KA) if the pairing has been already carried out, if not,

- searching for a free location (PDT) among the locations reserved for the pairing data in the first device (MS) and in this case,

- initiating a pairing procedure by transmitting a cryptogram (CY) contained in the second device (MH), and containing an identifier (SN) belonging to this device, this cryptogram being encrypted by a secret key (k) of the first device,

- decrypting this cryptogram (CY) within the first device and extracting from this cryptogram the identifier (SN) of the second device ,

- generating a pairing key (KA) based on this identifier,

- storing in the first device (MS) the pairing data with the second device.

2. Method according to claim 1, characterized in that the pairing key (KA) is based on the identifier (SN) of the second device and on the data of the first device (MS).

3. Method according to claims 1 or 2, characterized in that the cryptogram (CY) is stored in the first device (MS) and encrypted with a secret key common to the second devices (MHKey).

4. Method according to claims 1 to 3, characterized in that each location (PDT) includes an activity counter (CPT) updated during every positive verification of the pairing based on this location, the search for the location to be replaced being determined by the value of the activity counter (CPT).

5. Method according to claims 1 to 4, characterized in that pairing is conditioned by the introduction of a secret code (PIN) transmitted to the first device and verified by said first device.

6. Method according to claim 5, characterized in that the secret code belongs to and is unique to each first device (MS).

7. Method according to claim 5, characterized in that the required secret code is different in each pairing.

8. Method according to claim 5, characterized in that it comprises the steps of:

- transmitting a unique identifier of the first device and a unique identifier of the second device to a management centre,

- verifying the conformity of this pairing and calculating by means of the management centre the corresponding secret code (PIN) on the basis of the two identifiers,

- transmitting this secret code to the second device,

- initiating the pairing and requesting the introduction of the secret code (PIN),

- calculating by means of the first device the necessary secret code on the basis of the identifiers of the first and second devices,

- comparing the calculated code with that which has been introduced by the user,

- accepting the pairing if the two codes are identical.

9. Method according to claim 8, characterized in that it comprises the steps of determining the new secret code on the basis of the two identifiers and of an index (N) that represents the number of pairings previously carried out, whereas the first device stores this index (N) in its memory.